AUSA: Mark Chasteen Telephone: (313) 226-9555

AO 106 (Rev. 04/10) Application for a Search Warrant Agent: Thomas Cardinali Telephone: (202) 536-9863

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

Case: 2:19–mc–51508
Assigned To : Friedman, Bernard A.
Assign. Date : 10/15/2019
Description: RE: SEALED MATTER (EOB)

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Instagram account "therealcrispye__", user ID : 259836719

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C § 371, 1344, 1343	Conspiracy, Bank Fraud, Wire Fraud
18 U.S.C § 1028A, 1029	Aggravated Identity Theft, Access Device Fraud

The application is based on these facts:

See attached AFFIDAVIT.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Thomas Cardinali - Special Agent
Printed name and title

Sworn to before me and signed in my presence and/or by reliable electronic means.

Date: October 15, 2019

Judge's signature

City and state: Detroit, Michigan

David R. Grand U. S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Thomas Cardinali, being duly sworn, hereby depose and state as follows:

I. Introduction and Agent Background

1. I am a Special Agent with the United States Secret Service assigned to the Detroit Field Office, and I have been employed since March, 2015. I am currently assigned to the Electronic Crimes Task Force. I have participated in numerous investigations involving counterfeiting, bank fraud, computer fraud and access device fraud.

2. The information contained in this affidavit is based on my training, experience, and participation in financial crimes and cyber investigations, as well as from personal observations during the course of this investigation. Information was also provided by law enforcement officers and others who have personal knowledge of the events and circumstances described herein.

3. I have been trained in methods and traits commonly associated in financial fraud. I have received specialized training regarding counterfeiting and fraud, including violations of Title 18 U.S.C § 1344 (bank fraud), as well as 18 USC § 1343 (wire fraud), § 1028A (aggravated identity theft), and § 1029 (access device fraud).

4. I make this affidavit in support of an application in support of a search warrant for information associated with Ezel McELROY's Instagram account "therealcrispye__", user ID : 259836719 (the SUBJECT ACCOUNT). The information to be searched is described in the following paragraphs and in Attachment A and is stored at premises owned, maintained, controlled, or operated by Facebook and Instagram, a social networking company headquartered in Menlo Park, California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook and Instagram to disclose to the government records and other information in its possession, pertaining to the subscriber or user associated with the SUBJECT ACCOUNT, and authorizing the government to search those records and information for evidence or instrumentalities related to violations of 18 U.S.C. § 371 (conspiracy), § 1344 (bank fraud), § 1343 (wire fraud), § 1028A (aggravated identity theft), and § 1029 (access device fraud).

PROBABLE CAUSE

Fraudulent Activity at Fifth Third Bank

5. USSS Special Agent Lariviere learned the following from Susan

Clayton, an investigator employed by Fifth Third Bank: Between March 8 and March 27, 2018, eight counterfeit checks totaling $38,319.12 were deposited into various customers' accounts, each typically in the amount of $4,765.13 and nominally drawn from Massachusetts Mutual Life Insurance account 67937 at Bank of America. Based on surveillance, the person making the deposits was not the account holder. The deposited funds were later withdrawn via point of sale debit card transactions.

6. Later, additional similar fraudulent transactions occurred at Fifth Third, using different counterfeit checks, but involving 71 customer accounts and deposits of 117 fraudulent checks in amounts between $4,000 and $5,000, totaling $556,118.09 deposited through July 9, 2018. Mark D. Hobson was one customer into whose accounts a counterfeit check was deposited.

7. Investigator Clayton reported that by October 16, 2018, a total of $940,125.92 in fraudulent checks had been deposited. Funds commonly were withdrawn at two check cashing stores in Detroit, including Boulevard Check Cashing and Woodward Check Cashing. Clayton identified Ezel McELROY as an individual involved in the counterfeit check fraud scheme. Clayton obtained a driver license

from Shirley Hamby, an investigator at Comerica Bank, and was able to use the bank footage from Fifth Third and compared it to a driver license that was recovered from McELROY after he attempted to pass a counterfeit check at Comerica Bank. Clayton further believed that many of the Fifth Third account holders and runners were recruited via Instagram by a user or users using a profile containing "therealcrispye."

8. As discussed below, although it appears that many witnesses believed the "therealcrispye" Instagram profile name included only a single underscore (i.e., "therealcrispye_"). It is difficult, based on visual observation alone, to determine the number of underscores in the profile name. Subsequent investigation, including information received from Instagram, has shown that the profile name has two underscores: therealcrispye__. Accordingly, "therealcrispye" is used in this affidavit to describe generally variations of the profile name described by witnesses.

Fraudulent Activity at Comerica Bank

9. SA Lariviere also received information from Shirley Hamby. On March 19, 23, 26, and 29, and April 11, 2018, deposits or attempted deposits were made of counterfeit checks in Comerica customer

accounts. Each one was in the amount of $4,765.13 nominally from Mass Mutual and drawn on Bank of America account 67937—the same account number used for some of the counterfeit checks deposited with Fifth Third bank. Each transaction was made using a different Comerica Bank customer's account and at a different location. Funds were withdrawn from the accounts within three days of the deposits on March 19, 23, and 26 and April 11, 2018.

10. Between May 7 and May 21, 2018, deposits of seven counterfeit checks were made into Comerica accounts, each in the amount of $4,972.33 and nominally drawn on Bank of America from Mass Life account 67937. Six of the seven deposits were made into an account of a different customer, and the deposits were made at five different locations. Funds usually were withdrawn from the accounts within 1–2 days. On May 11, 2018, an attempted deposit of a counterfeit check in the amount of $4,972.33, nominally drawn on Bank of America from Mass Life account 67937, was made at a Comerica Bank location. The person who attempted to make the deposit fled the location, leaving the check behind.

11. On June 20 and June 21, 2018, three separate deposits or attempted deposits of counterfeit checks drawn on Sterling Bank and Trust,

account 67937, from CMAI Industries, each for $4,831.70, were deposited into a Comerica account in the name of B.B. Each deposit was made at a different Comerica Bank branch location. On June 21, 2018, ATM withdrawals totaling $4,500 were made at Boulevard Check Cashing in Detroit. Another ATM withdrawal for $320 was made at an ATM in Detroit. On June 22, 2018, B.B. went to a Comerica Bank location in Oak Park and attempted to withdraw $2,000.00.

12. B.B. told Shirley Hamby that she replied to an Instragram message: "if you have a bank account and would like to earn a few extra bucks . . . hit me up" from Instagram profiles BIIGTAE and therealcrispye. B.B. stated she did not know who BIIGTAE was, but therealcrispye belonged to Ezel McELROY, with whom she had attended Oak Park High School. The person associated with the @BIIGTAE profile came to B.B.'s home, and she gave him her ATM card and account number.

13. On June 26 and July 6, 2018, additional deposits of counterfeit checks drawn on Sterling Bank & Trust account 67937 in the amount of $4,831.70 were deposited into the Comerica bank accounts of two other customers. Withdrawals of funds totaling $4,800 and $2,500

were made from the two accounts within days of the deposits.

Fraudulent Activity at PNC Bank

14. On October 17, 2018, PNC Bank Investigator Carol Crane contacted USSS Special Agent Tyler Bennett and Special Agent Lariviere to provide information regarding an organized check fraud ring involving counterfeit life insurance checks. Crane stated that from April 9, 2018, to September 27, 2018, a total of 88 transactions occurred involving the depositing of counterfeit checks into 59 checking accounts for the amount of $799,231.58. With some exceptions, the checks ranged from $4,200.00 to $9,938.37. A total of $213,187.87 was withdrawn from the 59 accounts. Multiple counterfeit checks that were deposited contained the same company name, check number and account numbers. Many of the checks that were deposited contained the same information as the checks deposited at Fifth Third and Comerica. Video surveillance showed that checks were deposited into individual accounts by the account holders themselves and members of the organized check fraud ring. Following the deposits, funds were depleted via point of sale debit card transactions, wire transfers and cash advances throughout the Detroit area. Ezel McELROY was identified as one of the individuals

associated with depositing the counterfeit checks and withdrawing funds from ATMs.

West Bloomfield Township Police Department
Investigation and Arrest of Ezel McELROY

15. I have reviewed police reports, as well as search warrant applications, from the West Bloomfield Township (Michigan) Police Department (WBPD), and the Huron Township (Michigan) Police Department, and SA Lariviere met with WBPD Detective Erik Hamilton.

16. In the course of an investigation into a home invasion and armed robbery that occurred on January 30, 2018 at 6072 Silverbrooke West in West Bloomfield Township, WBPD determined that Ezel McELROY and his brother Blake Benford lived at that location. K.P. was a suspect in the home invasion and armed robbery. K.P. told WBPD detectives that Ezel McELROY used K.P.'s paycheck from Covenant Construction to create counterfeit checks.

17. Detective Hamilton interviewed K.P. on February 5, 2018. K.P. stated that he knows Ezel McELROY. About one month prior to the interview, K.P. received a direct message from McELROY through Instagram. McELROY inquired about K.P.'s JP Morgan Chase bank account and asked if K.P. wanted to make money. McELROY asked

for K.P.'s bank card, personal identification number, and online banking login so McELROY could deposit a "QuickPay" of $2,000–$3,000 into K.P.'s account. QuickPay is a mobile banking feature that allows users to deposit checks into their accounts remotely. McELROY said he would need K.P.'s bank card for a day or two, and K.P. would receive $500 for letting McELROY use the account. K.P. met McELROY at a gas station in Southfield, Michigan on January 1, 2018, and gave McELROY his bank card and online banking information. A few days later, McELROY told K.P. the QuickPay did not go through.

18. Around January 19-20, 2018, McELROY asked KP if he knew anyone with a bank account because KP's account was not "poppin."

19. K.P. stated a "Chris Financial" check in his account was from his employer Covenant Construction. K.P. thought McELROY found it while signed into his account. McELROY told K.P. he "remade" the check using account and routing numbers on K.P.'s check. McELROY told K.P. he was writing checks of $4,700 and making them payable to random people who were then "dropping" the checks into their accounts. Detective Hamilton reviewed a report from the Clinton Township Police Department in which the owner of Covenant

Construction reported that he had been informed by Christian Financial that a number of fraudulent checks had been cashed.

20. K.P. heard that McELROY downloaded a program that contains different formats for checks so he just had to input names and account numbers. K.P. recalled seeing a laptop computer connected to a printer inside McELROY's residence at 6072 Silverbrooke West that McELROY used to print checks. McELROY asked K.P. if he could get check paper and magnetic ink.

21. K.P. identified Instagram account therealcrispye as belonging to Ezel McELROY.

22. On February 6, 2018, Detective Hamilton reviewed an Instagram account therealcrispye and saw photographs of a black male consistent with Ezel McELROY. On February 6, therealcrispye posted "Who got a 700+ credit score and wanna make 5,000" and "who got a 600+ credit score and wanna make 3-5k."

23. On February 9, 2018, officers from the WBPD went to 6072 Silverbrooke West to execute a search warrant obtained from the 48th District Court. As they approached, officers saw an occupied Nissan Pathfinder running at the curb in front. Mark Hobson was walking from the direction of the apartment. When asked where he was

coming from, Hobson indicated he had come from a nearby apartment and stated he had not come from 6072. Based on tracks in newly fallen snow, it appeared Hobson had come from the entry door of 6072, not the apartment he indicated. Ezel McELROY was seated in the driver's seat of the Pathfinder. Another person, Mack C., was in the front passenger seat. A query showed the Pathfinder was listed as stolen by the Wayne County Airport Authority on February 2, 2018.

24. Ezel McELROY and Mack C. were arrested and transported to the WBPD station. McELROY was searched and found to be in possession of a Huntington Bank credit card bearing the name of N.B. and a card number ending in -1482.

25. Detective Runsat of the WBPD searched the Pathfinder and found: a Huntington Bank deposit receipt dated February 8, 2019, in the amount of $4,784.43 into account ending in -0315; a transaction record receipt dated 2/9/18 at 02:48 hours with card ending in -1482; a fraudulent Safeco Insurance Company check #82349 in the amount of $4,784.43 and dated January 6, 2018, made payable to Z.T.; and a birth certificate and traffic citation for Mark Hobson.

26. Detective Hamilton spoke with Huntington Bank investigator Jason Meggie, who stated that N.B. had an account at Huntington Bank

ending in 0315 and a deposit of $4,784.43 was made into N.B.'s account on February 8, 2018, which was not consistent with N.B.'s everyday banking activity. Detective Hamilton spoke with N.B., who reported that she lost her Huntington Bank debit card approximately two days earlier. Later, in June 2018, N.B. told Detective Hamilton that she received a text message from an unknown number asking about her debit card. She spoke with the person who sent the text and agreed to give her debit card so they could deposit a check. Shortly after that, two tall black males arrived at her home and she gave them her debit card and PIN.

27. Detective Hamilton reviewed an Apple iPhone belonging to Mack C. on February 13, 2018, and found texts, emails and photographs containing names, addresses, accounts, account login information, and transactions at several different banks. Detective Hamilton also found:

a. A text conversation in which a phone number ending in -5446 sent several pictures containing the personal identifying information of different people;

b. A picture of N.B.'s address and Huntington Bank login and password, received on February 6, 2018 (messages around the picture discussed when to pick up N.B.'s card and depositing a

check);

c. A photograph dated January 14, 2018, showing an unknown online bank account with balances of $5,842.56 and $20,000.00 (It appeared the photograph was posted to therealcrispye's Instagram page where written across the photograph is, "My lil nigga Mack go so crazy.");

d. A photograph dated 1/10/18 from mcelroyezel@icloud.com where McELROY sent Mack C. a text message via icloud with a username and password for D.L., as well as D.L.'s address and county of residence;

e. In an Instagram album, several photographs soliciting someone with a bank account who wants to make money.

28. Officers of the WBPD searched 6072 Silverbrooke West on February 9, 2018, pursuant to the search warrant and found documents associated with Ezel McELROY in the southeast bedroom. In that bedroom, officers also found:

a. Several mobile phones, including a black Apple iPhone with IMI #356769087236816, currently in the custody of the United States Secret Service in Detroit, Michigan);

b. a Huntington MasterCard in the name of D.H.; and

c. Christian Financial cards in the name of A.Z. and M.P.

29. In the dining room of 6072 Silverbrooke West, officers found a HP laptop computer with a camouflage pattern, a HP laser jet printer, two printed checks, and a box of blank payroll checks with no checking account information printed on the face. In the living room, officers found a rose-colored Apple MacBook computer, serial number C02VG2HFHH27.

30. WBPD Detective St. Germaine contacted D.H., whose Christian Financial card was found in Ezel McELROY's bedroom. D.H. stated he did not give any other person permission to have his bank card. D.H. stated his account was cancelled after a check was cashed fraudulently on his account.

31. On February 10, 2018, Detective Hamilton interviewed D.B., who was sleeping on the living room couch when officers entered 6072 Silverbrooke West on February 9. D.B. stated the following:

a. Ezel McELROY, Blake Benford, and Moses McElroy all used the camouflage laptop computer officers found on the dining room table.

b. D.B. had seen checks on the printer but could not say who printed them because multiple people use the printer.

c. After checks are printed, they are placed into an envelope to make them look like payroll checks.

d. After a check is cashed, Ezel McELROY and Benford take half of the money and the person who cashed it receives the other half. The check will then be "dropped" a second time, and split again, so that Ezel McELROY and Benford receive the full amount of $4,783.43.

e. The most commonly used banks are Bank of America, Huntington Bank, and Michigan First Credit Union, but they will use all banks and have been pretty successful.

32. On or about February 9, 2018, WBPD Detective St. Germaine contacted A.Z., whose Christian Financial card was found in Ezel McELROY's bedroom. At that time, A.Z. stated he did not give any other person permission to have his bank card and that an unknown person applied for another card in his name without his knowledge and tried to change his email. Detective Hamilton spoke with A.Z. again on February 16, 2018. A.Z. said a few weeks earlier an acquaintance, B.W., advertised on his Snapchat account that he was looking for anyone with an active bank account who wanted to make money. A.Z. met with B.W., who pressured him into giving B.W. his

Christian Financial debit card and access to his bank account to cash a check. A few days later, Christian Financial informed A.Z. that a fraudulent check had been deposited into his account.

33. On or about February 20, 2018, Detective Hamilton did a preview of the camouflage HP laptop found in the dining room of 6072 Silverbrooke West, and found that the Checksoft program had been installed. A Google search showed that Checksoft is used to design and print personal, business, and payroll checks.

34. On April 9, 2018, Detective Hamilton reviewed the rose-colored Apple MacBook found in the living room of 6072 Silverbrooke West. The MacBook contained a user profile for Ezel McELROY that was password locked. Hamilton used a password previously provided by McELROY and unlocked the computer. The email and messaging applications automatically opened. Among other evidence of identity theft and bank fraud, Detective Hamilton saw:

a. Messages to or from two different telephone numbers in which over 300 customer profiles for T-Mobile accounts containing personally identifiable information, including name, address, DOB, phone number, username, password, and some complete social security numbers were exchanged;

b. A February 5, 2018, screen shot of a sample State of Wisconsin check;

c. A February 5, 2018 screen shot of a Bank of America online account showing a deposit of a State of Wisconsin Income Tax Refund check payable to T.W. in the amount of $1,301.64;

d. A photograph dated February 6, 2018, showing a check in the amount of $980.56 payable to T.W., drawn on the TD Bank account of Future Project DD Department;

e. A Gmail account for crispygang24@gmail.com in the internet history.

35. On April 10, 2018, Detective Hamilton spoke with a manager at TD Bank, who advised that Future Project DD Department had experienced fraudulent checks being cashed, leading to its account being frozen. Detective Hamilton subsequently received a phone call from A.G., who identified himself as the owner of Future Project, and who confirmed his business had experienced fraudulent checks in Detroit, Michigan and Orlando, Florida, and stated neither he nor his company had employed T.W. Detective Hamilton located a phone number for T.W. and spoke with a female who identified herself as T.W. T.W. said 2–3 months earlier she experienced fraud on her Bank

of America account where three fraudulent checks were deposited into her account. T.W. at first denied involvement, then said she was propositioned by a friend, B.M., about giving her online banking information and debit card and was promised $1,000 for the use of her account. B.M. was going to give her information to a friend who would deposit checks into her account.

36. On April 18, 2018, Detective Hamilton examined the camouflage HP laptop found in the dining room at 6072 Silverbrooke West on February 9, 2018. The laptop had nine user accounts, including one for "Crisp" with a full username of "crispy e cg 24". On January 15, 2018, the user Crisp downloaded CheckSoft V14.0.1 business edition, as well as the CheckDesigner.pdf user guide. An HP printer was installed on the computer. Google searches using the Crisp user profile included: "what sites let you pay with checking," "check fraud protection," "genuine original waterstamp," "original genuine check," "Safeco Insurance," and "check fraud protection symbol."

37. On August 21, 2018, 48th District Court (Michigan) Judge Barron found probable cause on a criminal complaint charging McELROY with one count of obtaining, possessing, or transferring personal identifying information with intent to commit identity theft and two

counts of financial transaction device fraud and signed a warrant for his arrest.

Arrest of Ezel McELROY and Mark Hobson by the Huron Township Police Department

38. On August 25, 2018, Officer Sheehan of the Huron Township (Michigan) Police Department stopped a Dodge Charger that was traveling southbound on I-275 at 105 miles per hour. Ezel McELROY was driving the Charger, and Mark Hobson was in the front passenger seat. McELROY and Hobson were arrested on outstanding warrants. At the time of his arrest, McELROY had in his possession an Apple iPhone, IMEI#354856093929633. Hobson had a Samsung Galaxy mobile phone, IMEI #359754071351554. Both phones currently are in the custody of the United States Secret Service.

39. Officers searched the Charger and found a bag on the passenger side floor, at Hobson's feet. The bag contained:

a. A card scanner capable of being Bluetooth linked to any Bluetooth capable smart phone for the purpose of reading and writing to cards from the phone;

b. A bank statement from Fifth Third showing four different checks payable to Hobson, all returned to Hobson due to

fraudulent activity. The statement showed the checks being cashed four consecutive days for approximately $4,900 each;

c. A statement showing Hobson's account overdrawn by approximately $14,000;

d. 13 credit cards. A magnetic strip scan showed that 10 of the cards had different numbers in the magnetic strip than showed on the face of the card, two did not scan, and one registered to Hobson and the strip matched the face.

40. In the trunk of the Charger, officers found:

a. An Amazon box containing several hundred blank checks in three different types with security features which can be found on counterfeit checks passed at Fifth Third, PNC, and Comerica banks;

b. A Chase bank card with no name and a Fifth Third Bank card in the name of a person other than McELROY or Hobson.

Southfield Police Department Arrest

41. I have also reviewed a report from the Southfield Police Department detailing an arrest of Ezel McELROY. On July 9, 2018, McELROY was arrested after officers observed him driving recklessly in a Dodge Charger SRT Hellcat. The report states that McELROY was the sole

occupant of the vehicle and an inventory search of the vehicle revealed seven credit cards belonging to seven different individuals in the center console. A Bank of America check nominally drawn on the account of DLanzo Plumbing and Sewer and payable to Ariana McDuffle for $14,525.09 was found in the glove compartment. A search incident to arrest revealed $5,961.76 in cash in McELROY's front left pocket. McELROY stated that he sells cars for his uncle and gets paid in cash.

42. The owner of the DLanzo Plumbing and Sewer Company, D.L., was contacted regarding the check found in McELROY's possession. D.L. said that he did not know Ariana McDuffle, the name payable on the check, and he contacted his bank to see if any checks were made payable to Ezel McELROY. D.L. discovered that none of the checks were made payable to McELROY, but over $25,000 in fraudulent checks had been cashed. On March 12, 2019, I spoke with D.L. and he stated the check is in fact counterfeit and it was not written by his company.

43. At the time of his arrest by the Southfield Police Department, McELROY had in his possession several bank debit cards in the name

of other people. Three of the cards were for accounts that were closed after a counterfeit check was deposited.

Other Facts Supporting Probable Cause

44. Mark Hobson opened a Fifth Third checking account on May 29, 2018. Four counterfeit checks were deposited into Hobson's account in the approximate amount of $4,800.00 each, starting on June 4, 2018, through June 7, 2018. Based on the bank security footage provided by Fifth Third Bank Investigator Clayton and a list of deposits into Hobson's account, I was able to determine he did not personally make any of the deposits. ATM camera footage shows McELROY withdrawing funds from Hobson's account.

45. On August 27, 2018, C.F., who was then 15 years old, went to the WBPD station and reported he lost his debit card a few weeks earlier and that someone impersonated him and withdrew money from his Chase account. C.F. later admitted to Detective Kase that he did not lose his card. Instead, he saw an Instagram post by "biigtae" advertising that he could make anyone $3,500 within a day. C.F. responded via direct message. The subject said C.F. would need to provide his personal information, bank account information, and a debit card where the money could be deposited into his account. C.F.

met with the person depicted on the Instagram account on July 16, 2018, and gave him his debit card. On July 17, 2018, $3,500 was deposited into C.F.'s account, and immediately withdrawn and transferred by an unknown person.

46. Detective Kase obtained photos of the fraudulent ATM withdrawal from a Chase investigator. C.F. did not recognize the person in the ATM photos, noting that his physical characteristics were not consistent with "biigtae." C.F. suggested he might be able to locate the subject from biigtae's Instagram followers. Detective Kase noted biigtae had over 44,000 followers, but C.F. provided the profile for therealcrispye within seconds. Detective Kase recognized the page as belonging to Ezel McELROY. Based on a vehicle license plate in a photo on the Instagram account and Gray's Secretary of the State photo, it appears biigtae belongs to Deonte Gray.

47. Ezel McELROY posts music videos on YouTube under the moniker Crispy E. For example, one video posted on November 18, 2018 and titled "Filthy Rich" lists the artist as "Crispy E (@Therealcrispye__)." In the video, McELROY states: "My lawyer just said the feds are watching me. S***, I don't give a f***, ain't no stopping me."

48. A post on the Instagram account biigtae by therealcrispye says "My

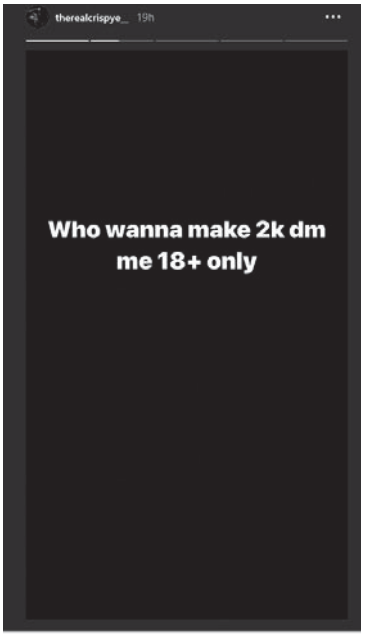
boy" and shows a photo of a black male wearing a gold chain with a "CRISPY E" pendant. SA Lariviere recognized the black male wearing the "CRISPY E" chain as McELROY. Huron PD took possession of the "CRISPY E" chain at the time of McELROY's arrest and subsequently turned it over WBPD were it remains in their custody.

49. Interviews conducted by Susan Clayton during this investigation identified T.T. who stated that therealcrispye. was the account used to coordinate the check fraud scheme between himself and McELROY. T.T. was interviewed by myself and SA Lariviere. T.T. stated he had seen a post by therealcrispye, in which he was offering people with bank accounts a way to make some money. T.T. stated that he approached McELROY at a gas station after seeing the post on Instagram. T.T. stated he turned over his account information to McELROY. T.T. stated a majority of the communication between himself and McELROY took place via Instagram and account therealcrispye. T.T. stated that all banking information username, password, debit PIN were turned over via therealcrispye. T.T. stated the card was given to McELROY in person.

50. The following are examples of images taken from the Instagram

profile therealcrispye__:

This image was obtained by WBPD and illustrates the use of Instagram to provide information about his conduct. Several of the user names who commented on the photo have been identified as accounts used to recruit individuals into the current check fraud scheme.



These photos were obtained by WBPD and show that McELROY used his Instagram account to flaunt large sums of cash and to recruit his followers for the fraud scheme.

Instagram

51. From my review of publicly available information provided by Instagram about its service, including Instagram's "Privacy Policy," I am aware of the following about Instagram and about the information collected and retained by Instagram.

52. Instagram owns and operates a free-access social-networking website of the same name that can be accessed at http://www.instagram.com. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application ("app") created by the company that allows users to access the service through a mobile device.

53. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various "tags" that can be used to search for the photo (e.g., a user made add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of "filters" or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on

posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also "like" photos.

54. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Instagram.

55. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user's full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.

56. Instagram allows users to have "friends," which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.

57. Instagram also allows users to "follow" another user, which means that they receive updates about posts made by the other user. Users may also "unfollow" users, that is, stop following them or block them, which prevents the blocked user from following that user.

58. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.

59. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.

60. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

61. For each user, Instagram also collects and retains information, called "log file" information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Instagram's servers automatically record is the particular web requests, any Internet Protocol ("IP) address associated with the request, type of browser used, any referring/exit web pages

and associated URLs, pages viewed, dates and times of access, and other information.

62. Instagram also collects and maintains "cookies," which are small text files containing a string of numbers that are placed on a user's computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user's interests.

63. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

64. Instagram also collects other data associated with user content. For example, Instagram collects any "hashtags" associated with user content (i.e., keywords used), "geotags" that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information.

65. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.

66. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user's account activity, IP log, stored electronic communications, and other data retained by Instagram, can indicate who has used or controlled the Instagram account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was accessed or used. For example,

as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Instagram "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner's state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

67. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to the SUBJECT ACCOUNT, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

Prior Instagram Warrant and Subsequent Investigation

68. On June 6, 2019, United States Magistrate Judge Majzoub signed a warrant to search and obtain information from an Instagram account with the user name "therealcrispye_" (with one underscore) and user ID 259836719 based on an application submitted by SA Lariviere. Upon receipt of the warrant, Facebook/Instagram informed SA Lariviere that they could not provide the requested information because the user name and the user ID did not match. The user ID requested belonged to a profile with two underscores (i.e., "therealcrispye__"). As described in SA Lariviere's application, witnesses described the "therealcrispye" profile as having a single

underscore (i.e., "therealcrispye_"). It is difficult to discern from visual observation the number of underscores in McELROY's "therealcrispye" username. SA Lariviere looked at McELROY's "therealcrispye" user name online and read it has having only one following underscore, and I believe that other people made the same error when reading or describing McELROY's user name. Through subsequent investigation, I have learned the Instagram account associated with McELROY is "therealcrispye__" (with two underscores) and user ID 259836719. Instagram provided account information for this account that included a verified telephone number of XXX-XXX-8696. According to a database of public and private records accessible to law enforcement, XXX-XXX-8696 is associated with Ezel McELROY and 6072 Silverbrook W in West Bloomfield, Michigan. This application is for a warrant to search Facebook/Instagram for information associated with the account or profile identified as "realcrispye__" (with two underscores) and user ID 259836719.

Information To Be Searched And Things To Be Seized

69. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A), by using the warrant to require Facebook/Instagram to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

Conclusion

70. Based on the forgoing, I request that the Court issue the proposed search warrant.

71. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

72. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Because the warrant will be served on Instagram, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

73. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the listed SUBJECT ACCOUNT and to search for evidence and instrumentalities related to violations of 18 U.S.C. § 371 (conspiracy), § 1344 (bank fraud), § 1343 (wire fraud), § 1028A (aggravated identity theft), and § 1029 (access device fraud). There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

Thomas Cardinali
Special Agent
United States Secret Service

Sworn to before me and signed in my presence and/or by reliable electronic means on October 15th, 2019

DAVID R. GRAND
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A:

Property To Be Searched

This warrant applies to information associated with the Instagram profile with username:

"therealcrispye__" user ID 259836719;

https://www.instagram.com/therealcrispye__/

that is stored at premises owned, maintained, controlled, or operated by Instagram, LLC, a company that is owned by Facebook, Inc. and headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things To Be Seized

I. Information to be disclosed by Instagram, LLC

To the extent that the information described in Attachment A is within the possession, custody, or control of Instagram, LLC, including any messages, records, files, logs, or information that have been deleted but are still available to Instagram, LLC, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Instagram, LLC is required to disclose the following information to the government **covering the dates of January 1, 2017, to the date of this warrant** for each account listed in Attachment A:

a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;

b. All past and current usernames associated with the account;

c. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

d. All activity logs including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;

e. All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;

f. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

g. All communications or other messages sent or received by the account;

h. All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content;

i. All photographs and images in the user gallery for the account;

j. All location data associated with the account, including geotags;

k. All data and information that has been deleted by the user;

l. A list of all of the people that the user follows on Instagram and all people who are following the user (*i.e.*, the user's "following" list and "followers" list), as well as any friends of the user;

m. A list of all users that the account has "unfollowed" or blocked;

n. All privacy and account settings;

o. All records of Instagram searches performed by the account, including all past searches saved by the account;

p. All information about connections between the account and third-party websites and applications; and,

q. All records pertaining to communications between Instagram, LLC and any person regarding the user or the user's Instagram account, including contacts with support services, and all records of actions taken, including suspensions of the account.

II. **Information to be seized by the government**

All information described above in Section I that constitutes evidence or instrumentalities of violations of 18 U.S.C. § 371 (conspiracy), § 1344 (bank fraud), § 1343 (wire fraud), § 1028A (aggravated identity theft), and § 1029 (access device fraud), including, for each username identified on Attachment A, information pertaining to the following matters:

a. the possession, manufacture, sale, or use of stolen/fraudulent accounts, including credit, debit, and other accounts that may be used to buy or sell things of value;

b. the purchase, sale, or use of items purchased with stolen/fraudulent accounts, including credit, debit, and any other accounts that may be used to buy or sell things of value;

c. the purchase, manufacture, sale, or use of stolen identities, including FICO reports, credit scores, and driver's licenses;

d. use or transfer of monetary instruments, including the laundering of money instruments, derived from items acquired from the use of stolen/fraudulent accounts and identities;

e. evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Instagram account owner;

f. evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation;

g. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

h. The identity of the person(s) who communicated with the user ID about matters relating to the possession, manufacture, sale, or use of stolen/fraudulent accounts and/or identities, the purchase or sale of items acquired from stolen/fraudulent accounts and/or identities, or money laundering, including records that help reveal their whereabouts.

AO 93 (Rev. 11/13) Search and Seizure Warrant

AUSA: Mark Chasteen Telephone: (313) 226-9555
Agent: Thomas Cardinali Telephone: (202) 539-9863

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Instagram account "therealcrispye__", user ID : 259836719	)	Case No.

Case: 2:19−mc−51508
Assigned To : Friedman, Bernard A.
Assign. Date : 10/15/2019
Description: RE: SEALED MATTER (EOB)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Michigan.
(identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

YOU ARE COMMANDED to execute this warrant on or before October 29, 2019 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: October 15, 2019 3:54 pm

Judge's signature

City and state: Detroit, Michigan David R. Grand U. S. Magistrate Judge
Printed name and title

File No. 2018R01616

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title